Data Protection Addendum

This Data Protection Addendum ("***Addendum***") is entered into as of the date of the last signature below, (the **"Effective Date"**), by and between the customer specified in the table below ("***Customer***") and Twilio Inc. ("***Twilio***").

Twilio Inc.	Customer: Cloud Paper Group Pty Ltd
Signature: DocuSigned by: Karyn Smith 155G18E1BFB4E4E4... Name: Karyn Smith Title: General Counsel and Secretary	Signature: DocuSigned by: David Eedle 60EEEAAFDE0C4C9... Name: David Eedle Title: Director Date Signed: 5/24/2018
Address: 375 Beale Street Suite 300 San Francisco, CA 94105, USA	Address: Level 1/3 Welling Street t Kilda VIC 3182 Australia
DPO/Contact for data protection enquiries Privacy Team privacy@twilio.com	DPO/Contact for data protection enquiries Name/Role: David Eedle Email: dpa@edsmart.com

This Addendum amends and supplements the Twilio Terms of Service ("***Agreement***"). If there is any conflict between this Addendum and the Agreement regarding the parties' respective privacy and security obligations, the provisions of this Addendum shall control.

I. Introduction

1. **Definitions.**

- "***controller***", "***processor***", "***data subject***", "***personal data***" and "***processing***" (and "***process***") shall have the meanings given in Applicable Data Protection Law;
- "***Applicable Data Protection Law***" shall mean: (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data; and (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("***General Data Protection Regulation***" or "***GDPR***").
- **"*Customer Account Data*"** shall mean personal data that relates to Customer's relationship with Twilio, including the names and/or contact information of individuals authorized by Customer to access Customer's Twilio account and billing information of individuals that Customer has associated with its Twilio account;
- **"*Customer Usage Data*"** shall mean data processed by Twilio for the purposes of transmitting, distributing or exchanging Customer Content; including data used to trace and identify the source and destination of a communication, such as individual data subjects' telephone numbers, data on the location of the device generated in the context of providing the Twilio Services, and the date, time, duration and the type of communication.
- **"*Customer Content*"** shall mean content exchanged by means of use of the Twilio Services, such as text, message bodies, voice and video media, images, and sound.
- **"*Privacy Shield Framework*"** shall mean the EU-US and/or Swiss-US Privacy Shield self-certification program operated by the US Department of Commerce.

- **"*Privacy Shield Principles*"** shall mean the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles).
- **"*Twilio Services*"** shall have the same meaning as in the Agreement.

2. **Relationship of the Parties.** The parties acknowledge and agree that with regard to the processing of Customer Content, Customer is a controller or processor, as applicable, and Twilio is a processor. With regard to the processing of Customer Account Data and Customer Usage Data, Customer is a controller or processor, as applicable, and Twilio is an independent controller, not a joint controller with Customer. Each party shall comply with its obligations under Applicable Data Protection Law, and this Addendum, when processing Personal Data.

II. Processor Obligations (Customer Content)

3. **Details of the processing.**

3.1 Subject Matter: Twilio's provision of the Twilio Services to Customer.

3.2 Purpose of the Processing: The purpose of the data processing under this Addendum is the provision of the Twilio Services as initiated by Customer from time to time.

3.3 Categories of Data: Data relating to individuals provided to Twilio via the Twilio Services, by (or at the direction of) Customer of Customer's end users.

3.4 Categories of Data Subjects: Data subjects may include Customer's customers, employees, suppliers and end users about whom data is provided to Twilio via the Twilio Services by (or at the direction of) Customer or by Customer's end users.

3.5 Duration of the Processing: As between Twilio and Customer, the duration of the data processing of Customer Content under this Addendum is necessarily determined by Customer.

4. **Customer Instructions.** Customer appoints Twilio as a processor to process Customer Content on behalf of, and in accordance with, Customer's instructions as set out in the Agreement and this Addendum, as otherwise necessary to provide the Twilio Services, or as otherwise agreed in writing ("***Permitted Purposes***"). Additional instructions outside the scope of the Agreement, this Addendum, or as otherwise needed to provide the Twilio Services may result in additional fees payable by Customer to Twilio for carrying out those instructions. Customer shall ensure that its instructions comply with all laws, regulations and rules applicable to the Customer Content, and that Twilio's processing of the Customer Content in accordance with Customer's instructions will not cause Twilio to violate any applicable law, regulation or rule, including Applicable Data Protection Law. Twilio agrees not to access or use Customer Content, except as necessary to maintain or provide the Twilio Services, or as necessary to comply with the law or other binding governmental order.

5. **Confidentiality of Customer Content and Responding to Third Party Requests.** In the event that any request, correspondence, enquiry or complaint from a data subject, regulatory or third party is made directly to Twilio in connection with Twilio's processing of Customer Content, Twilio shall promptly inform Customer providing details of the same, to the extent legally permitted. Unless legally obligated to do so, Twilio shall not respond to any such request, inquiry or complaint without Customer's prior consent except to confirm that the request relates to Customer to which Customer hereby agrees.

6. **Confidentiality Obligations of Twilio Personnel.** Twilio will ensure that any person it authorizes to process the Customer Content shall protect the Customer Content in accordance with Twilio's confidentiality obligations under the Agreement.

7. **Subcontracting.** Customer consents to Twilio engaging third party sub-processors to process Customer Content for Permitted Purposes provided that:

7.1 Twilio maintains an up-to-date list of its sub-processors at https://www.twilio.com/legal/sub-processors/, which as of May 2018 shall contain a mechanism to subscribe to notifications of new sub-processors. Customer shall subscribe, and if Customer subscribes, Twilio shall provide details of any change in sub-processors at least ten (10) days prior to any such change;

7.2 Twilio imposes data protection terms on any sub-processor it appoints that require it to protect the Customer Content to the standard required by Applicable Data Protection Law; and

7.3 Twilio remains liable for any breach of this Addendum that is caused by an act, error or omission of its sub-processor.

Customer may object to Twilio's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is in writing and based on reasonable grounds relating to data protection. In such event, the parties shall discuss commercial reasonably alternative solutions in good faith. If the parties cannot reach resolution, Twilio will either not appoint or replace the sub-processor or, if this is not possible, Customer may suspend or terminate the Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination).

8. **Data Subject Rights.** As part of the Twilio Services, Twilio provides Customer with a number of self-service features, including the ability to delete, retrieve, or restrict use of Customer Content, which may be used by Customer to assist in its obligations under Applicable Data Protection Law with respect to responding to requests from data subjects. In addition, Twilio will provide reasonable additional and timely assistance (at Customer's expense) to the extent the self-service features of the Twilio Services do not sufficiently enable Customer to comply with its data protection obligations with respect to data subject rights under Applicable Data Protection Law.

9. **Impact Assessments and Consultations.** On or after May 25, 2018, if Twilio believes or becomes aware that its processing of Customer Content is likely to result in a high risk to the data protection rights and freedoms of data subjects, Twilio shall inform Customer and provide reasonable cooperation to Customer (at Customer's expense) in connection with any data protection impact assessment or consultations with supervisory authorities that may be required under Applicable Data Protection Law.

10. **Return or Deletion of Customer Content.** The Twilio Services provide Customer with the capability to obtain a copy of its Customer Content by way of the API and/or console and delete the same. Accordingly, following termination or expiry of the Agreement, Twilio will provide a reasonable opportunity for Customer to obtain a copy of its Customer Content and delete the same. This requirement shall not apply to the extent that Twilio is required by law to retain some or all of the Customer Content, or to Customer Content it has archived on back-up systems, which Twilio shall securely isolate and protect from any further processing except to the extent required by law.

11. **Audit Obligations.**

    11.1 Twilio's Audit Program: The parties acknowledge that Customer must be able to assess Twilio's compliance with its obligations under Applicable Data Protection Law, insofar as Twilio is acting as a processor on behalf of Customer. Twilio uses external auditors to verify the adequacy of its security measures with respect to its processing of Customer Content. Such audits are conducted at least annually, are performed at Twilio's expense by independent third party security professionals at Twilio's selection, and result in the generation of a confidential audit report. A list of Twilio's certifications and/or standards for audit as of the date of this Addendum can be found at https://www.twilio.com/security.

    11.2 Customer Audit: Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Twilio shall make available to Customer a copy of Twilio's most recent audit report(s) generated as described in section 11.1 (Twilio's Audit Program), as applicable. Customer further agrees that any such audit reports meet Customer's audit requirements, and Customer agrees to exercise any right it may have to conduct an inspection or audit (including under Standard Contractual Clauses, as applicable) by instruction to Twilio to carry out the audit described above in Section 11.1 (Twilio's Audit Program). If Customer wishes to change this instruction, then Customer must send a written request to Twilio specifying the requested change. If Twilio declines the request to change the instruction, Customer may terminate the Agreement and this Addendum. If the Standard Contractual Clauses apply, nothing in this Section 11 (Audit Obligations) varies or modifies the Standard Contractual Clauses nor affects the supervisory authorities' or data subjects' rights under the Standard Contractual Clauses.

12. **Violations of Applicable Data Protection Law.** On or after May 25, 2018, Twilio will inform Customer if it becomes aware or reasonably believes that Customer's data processing instructions violate Applicable Data Protection Law.

III. Controller Obligations (Customer Account and Usage Data)

13. **Purpose Limitation.** Twilio shall process Customer Account Data and Customer Usage Data in accordance with Applicable Data Protection Law and consistent with its Privacy Notices as posted on its publicly-available website and/or the Agreement.

14. **Cooperation and Data Subject Rights.** In the event that either party receives: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Customer Account Data and Customer Usage Data; (collectively, "***Correspondence***") then, where such Correspondence relates (or also relates) to processing conducted by the other party, it shall promptly inform the other party and the parties shall cooperate in good faith as necessary to respond to such Correspondence and fulfil their respective obligations under Applicable Data Protection Law.
15. **Transparency.** The parties acknowledge that Twilio does not have a direct relationship with Customer's end users whose personal data Twilio may process in connection with Customer's use of the Twilio Services. Customer shall be responsible for ensuring its end users are provided adequate notice of Twilio's processing activities, including with respect to Customer end user data for which Twilio acts as a controller, and shall make available to end users a privacy notice that fulfills the requirements of Applicable Data Protection Law. Twilio agrees to provide Customer with sufficient information regarding its processing activities to allow Customer to provide such notice.

IV. Security

16. **Security Measures.** Twilio has implemented and will maintain appropriate technical and organizational measures to protect Customer Account Data, Customer Usage Data, and Customer Content (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the such data (a "***Security Incident***"). Measures to protect Customer Content from a Security Incident are described at https://www.twilio.com/security.

    16.1 Determination of Security Requirements: Customer acknowledges that the Twilio Services include certain features and functionalities that Customer may elect to use that impact the security of the data processed by Customer's use of the Twilio Services, such as, but not limited to, encryption of voice recordings and availability of multi-factor authentication on Customer's Twilio account. Customer is responsible for reviewing the information Twilio makes available regarding its data security, including its audit reports, and making an independent determination as to whether the Twilio Services meet the Customer's requirements and legal obligations, including its obligations under this Addendum. Customer is further responsible for properly configuring the Twilio Services and using available features and functionalities to maintain appropriate security in light of the nature of the data processed by Customer's use of the Twilio Services.

    16.2 Security Incident Notification - Customer Content: Twilio shall, to the extent permitted by law, promptly notify Customer of any Security Incident of which Twilio becomes aware. To the extent such Security Incident is caused by a violation of the requirements of this Addendum by Twilio, Twilio shall make reasonable efforts to identify and remediate the cause of such Security Incident. Twilio shall provide reasonable assistance to Customer in the event that Customer is required under Applicable Data Protection Law to notify a supervisory authority or any data subjects of the Security Incident.

    16.3 Security Incident Notification - Customer Usage Data: If Twilio becomes aware of a confirmed Security Incident involving Customer Usage Data containing the personal data of data subjects with whom Twilio does not have a direct relationship, for example Customer's end users, and Twilio determines that the incident must be reported to a regulatory authority, Twilio will notify the Customer of the incident and of its obligation and intent to notify the regulatory authority. If the impacted data subjects are required to be notified of the Security Incident, Customer will provide reasonable assistance to Twilio to effectuate appropriate notice to the impacted data subjects.

V. International Transfers of Data

17. Customer acknowledges that, as of the Effective Date of this Addendum, Twilio's primary processing facilities are in the United States. To the extent that Customer's use of the Twilio Services requires transfer of personal data out of the European Economic Area ("***EEA***"), Twilio will take such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) transferring the Customer Account Data, Customer Content or Customer Usage Data to a recipient in a country that the European Commission has decided provides adequate protection for personal data, to a recipient that has

achieved binding corporate rules authorization in accordance with Applicable Data Protection Law, or to a recipient that has executed Standard Contractual Clauses adopted or approved by the European Commission.

In the event that the Twilio Services are covered by more than one transfer mechanism, the transfer of personal data will be subject to a single transfer mechanism in accordance with the following order of precedence: (i) Twilio's binding corporate rules; (ii) Twilio's EU-US and Swiss-US Privacy Shield Framework self-certifications; and (iii) the Standard Contractual Clauses as set forth in Exhibit 1 to this Addendum.

17.1 Twilio BCRs: Should Twilio achieve binding corporate rules ("***BCRs***") authorization in accordance with Applicable Data Protection Law, the parties agree that Twilio will process Customer Account Data, Customer Content and Customer Usage Data in accordance with those binding corporate rules. The parties further agree that the BCRs will become the lawful transfer mechanism of Customer Account Data, Customer Content and Customer Usage Data from the EEA to Twilio in the United States, or any other non-EEA Twilio entity subject to the binding corporate rules, and will supersede any other lawful transfer mechanism previously in place.

17.2 Privacy Shield: The parties further agree that the Privacy Shield Framework will be the lawful transfer mechanism of Customer Account Data, Customer Content and Customer Usage Data from the EEA or Switzerland to Twilio in the United States, only to the extent such transfer is not covered by the Twilio BCRs pursuant to Section 17.1 (Twilio BCRs) of this Addendum. Twilio represents that it is self-certified to the Privacy Shield Framework and agrees, with respect to Customer Account Data, Customer Content and Customer Usage Data that it shall comply with the Privacy Shield Principles when handling any such data. To the extent that Customer is also self-certified to the Privacy Shield, Twilio further agrees:

17.2.1 To provide at least the same level of protection to such data as is required by the Privacy Shield Principles;

17.2.2 To notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles; and

17.2.3 Upon notice, including under Section 17.2.2 above, to work with Customer to take reasonable and appropriate steps to stop and remediate any unauthorized processing of Personal Data.

17.3 Standard Contractual Clauses: The parties further agree that the Standard Contractual Clauses in Exhibit 1 to this Addendum will apply to personal data within Customer Content that is transferred from the European Economic Area and/or Switzerland to outside the European Economic area and Switzerland, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive) and (ii) not covered by the Twilio BCRs pursuant to Section 17.1 (Twilio BCRs) of this Addendum or by the Privacy Shield certification pursuant to Section 17.2 (Privacy Shield) of this Addendum.

VI. Miscellaneous

18. **Entire Agreement; Conflict**. This Addendum supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations and agreements, oral and written, with regard to the subject matter of this Addendum, including any prior data processing addenda entered into between Twilio and Customer. If there is any conflict between this Addendum and any agreement, including the Agreement, the terms of this Addendum shall control.

EXHIBIT 1

Standard Contractual Clauses

European Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Data transfer agreement between

Customer who has executed the above Addendum,
hereafter "data exporter"

And

Twilio Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105 USA
Tel.: (877) 889-4546; fax (415) 376-8596; email: privacy@twilio.com
hereinafter "data importer;"

each a "party"; together "the parties".

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a

result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer[1]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.
   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[2]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12
Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

DATA EXPORTER

Authorised Signature: DocuSigned by: David Eedle 60EEEAAFDE0C4C9...

Name: David Eedle

Title: Director

DATA IMPORTER (Twilio Inc.)

Authorised Signature: DocuSigned by: Karyn Smith 55C18E1BFB4E4E4...

Name: Karyn Smith

Title: General Counsel and Secretary

[2] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is the entity identified as the "data exporter" in the Twilio Data Protection Agreement, and the user of Twilio Inc.'s services.

Data importer
The data importer is Twilio Inc., a provider of business communications services that enable communications features and capabilities to be embedded into web, desktop and mobile software applications.

Data subjects
The personal data transferred concern the following categories of data subjects:

Data exporter's customers and end-users. The data importer will receive any personal data in the form of Customer Content that the data exporter instructs it to process through its cloud communications products and services. The precise personal data that the data exporter will transfer to the data importer is necessarily determined and controlled solely by the data exporter.

Categories of data
The personal data transferred concern the following categories of data (please specify):

Customer Content: content exchanged by means of use of Twilio's Services, such as text, message bodies, voice and video media, images, and sound

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

Twilio Inc. does not intentionally collect or process any special categories of data in the provision of its products and/or services.

However, special categories of data may from time to time be inadvertently processed by Twilio Inc. where the data exporter or its end users choose to include this type of data within the communications it transmits using Twilio Inc.'s products and/or services. As such, the data exporter is solely responsible for ensuring the legality of any special categories of data it or its end users choose to process using Twilio Inc.'s products and/or services.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

Provision of programmable communication products and services, primarily offered in the form of APIs, on behalf of the data exporter, including transmittal to or from data exporter's software application from or to the publicly-switched telephone network (PSTN) or by way of other communications networks.

Storage on Twilio Inc.'s network.

DATA EXPORTER

Authorised Signature: DocuSigned by: David Eedle 60EEEAAFDE0C4C9...

Name: David Eedle

Title: Director

DATA IMPORTER (Twilio Inc.)

Authorised Signature: DocuSigned by: Karyn Smith 55C18E1BFB4E4E4...

Name: Karyn Smith

Title: General Counsel and Secretary

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or documentation/legislation attached):

See https://www.twilio.com/security for information and details regarding technical and organisational measures implemented by Twilio.

DATA EXPORTER

Authorised Signature: DocuSigned by: David Eedle 60EEEAAFDE0C4C9...

Name: David Eedle

Title: Director

DATA IMPORTER (Twilio Inc.)

Authorised Signature: DocuSigned by: Karyn Smith 55C18E1BFB4E4E4...

Name: Karyn Smith

Title: General Counsel and Secretary

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

This Appendix does not vary or modify the Clauses. It sets out the parties' interpretation of their respective obligations under specific Clauses identified below. As permitted by Clause 10 of these Clauses, the purpose of the interpretations is to enable the parties to fulfil their obligations in practice.

Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.
3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the noncompliance ("**Cure Period**").
4. If after the Cure Period the data importer has not or cannot cure the noncompliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(j): Disclosure of sub-processor agreements:

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward sub-processor agreement it concludes under the Clauses to the data exporter.
2. The parties further acknowledge that, pursuant to sub-processor confidentiality restrictions, data importer may be restricted from disclosing onward sub-processor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any sub-processor it appoints to permit it to disclose the sub-processor agreement to data exporter.
3. Even where data importer cannot disclose a sub-processor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such sub-processing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in data importer's Terms of Service in effect as of the date of execution of these Clauses or other written or electronic agreement for data exporter's use and purchase of data importer's products and services. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward sub-processing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC" the data exporter may provide a general consent to onward sub-processing by the data importer.
2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward sub-processors. Such consent is conditional on data importer's compliance with

the requirements set out below, which collectively ensure that the onward sub-processor will provide adequate protection for the personal data that it processes:

a) any onward sub-processor must agree in writing:

I. to only process personal data in the European Economic Area or another country that the European Commission has formally declared to have an "adequate" level of protection in accordance with the requirements of EU Directive 95/46/EC; or

II. to process personal data on terms equivalent to these Clauses or pursuant to a Binding Corporate Rules approval granted by competent European data protection authorities and whose scope extends to transfers of personal data from the territories in which the data exporter is established; and

b) data importer must restrict the onward sub-processor's access to personal data only to what is strictly necessary to perform its subcontracted data processing services to data importer (which shall be consistent with the instructions issued to data importer by data exporter) and data importer will prohibit the onward sub-processor from processing the personal data for any other purpose.

DATA EXPORTER

Authorised Signature: DocuSigned by: David Eedle 60EEEAAFDE0C4C9...

Name: David Eedle

Title: Director

DATA IMPORTER (Twilio Inc.)

Authorised Signature: DocuSigned by: Karyn Smith 55C18E1BFB4E4E4...

Name: Karyn Smith

Title: General Counsel and Secretary